We claim:

1. A computer program product for digitally notarizing a collection comprising a plurality of data streams, the computer program product embodied on one or more computer-usable media and comprising:

computer-readable program code means for computing a hash value over each of the plurality of data streams, wherein each data stream is created by a different application processing component;

computer-readable program code means for combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a combination data block;

computer-readable program code means for hashing the combination data block;

computer-readable program code means for digitally signing the hashed combination data block with a private cryptographic key, wherein the private cryptographic key and a public cryptographic key which is cryptographically associated therewith represent a digital notary; and

computer-readable program code means for providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the collection plurality of data streams, wherein the digital notarization cryptographically seals contents of the collection of data streams.

2. The computer program product according to Claim 1, wherein:

the computer-readable program code means for combining and the computer-readable program code means for hashing operate on pairs of (hash values, identifiers), one pair for each of the plurality of data streams;

the computer-readable program code means for digitally signing digitally signs each of the hashed pairs; and

the computer-readable program code means for providing provides the digitally signed hashed pairs, along with the hashed pairs, as the digital notarization.

3. The computer program product according to Claim 1, wherein:

the computer-readable program code means for computing a hash operates periodically, upon expiration of an elapsed time value, to compute a hash value over each of a plurality of segments of each data stream;

the computer-readable program code means for combining, the computer-readable program code means for hashing, and the computer-readable program code means for digitally signing all operate on the periodically-computed hash values for each data stream; and

the computer-readable program code means for providing provides the digitally signed periodically-computed hash values, along with the periodically-computed hash values, as the digital notarization; and

further comprising computer-readable program code means for inserting an identification of a time corresponding to each of the periodically-computed hash values at appropriate locations within each of the data streams.

4 The computer program product according to Claim 3, wherein the computer-readable program code means for inserting uses MPEG-4 synchronization timestamping.

5. The computer program product according to Claim 3, wherein authenticity and integrity of each of the segments is independently verifiable.

6. The computer program product according to Claim 3, further comprising:

computer-readable program code means for extracting selected ones of the segments of the data streams; and

computer-readable program code means for verifying integrity of the extracted selected ones using the public cryptographic key of the digital notary.

7. The computer program product according to Claim 3, further comprising:

computer-readable program code means for authenticating, by the digital notary, each of the application processing components;

computer-readable program code means for extracting selected ones of the segments of the data streams; and

computer-readable program code means for verifying authenticity of the extracted selected ones using the public cryptographic key of the digital notary and the digital notarization.

8. The computer program product according to Claim 1, further comprising:

computer-readable program code means for adding an additional data stream to the collection, wherein the additional data stream comprises the digital notarization.

9. The computer program product according to Claim 7, wherein the identifiers serve to identify data streams from each of the authenticated application processing components.

10. The computer program product according to Claim 1, further comprising computer-readable program code means for authenticating each of the application processing components using the unique identifier thereof, along with a digital signature of the unique identifier that is created using a private key of the application processing component.

11. The computer program product according to Claim 10, wherein inclusion of the unique identifiers within the combination data block allows concluding that each data stream in the collection was created by an authentic application processing component if operation of a verification process succeeds, wherein the verification process further comprises:

using the public cryptographic key of the digital notary to decrypt the digitally signed hashed combination data block, yielding a new version of the hashed combination data block and a new version of the combination data block;

computing a new hash over the new version of the combination data block; and

determining whether the new hash is identical to the new version of the hashed combination data block.

12. The computer program product according to Claim 11, wherein successful operation of the verification process also allows concluding that the data streams in the collection have not been altered.

13. A system for digitally notarizing a collection comprising a plurality of data streams, comprising:

means for computing a hash value over each of the plurality of data streams, wherein each data stream is created by a different application processing component;

means for combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a combination data block;

means for hashing the combination data block;

means for digitally signing the hashed combination data block with a private cryptographic key, wherein the private cryptographic key and a public cryptographic key which is cryptographically associated therewith represent a digital notary; and

means for providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the collection of data streams, wherein the digital notarization cryptographically seals contents of the collection of data streams.

14. The system according to Claim 13, wherein:

the means for combining and the means for hashing operate on pairs of (hash values, identifiers), one pair for each of the plurality of data streams;

the means for digitally signing digitally signs each of the hashed pairs; and

the means for providing provides the digitally signed hashed pairs, along with the hashed pairs, as the digital notarization.

15. The system according to Claim 13, wherein:

the means for computing a hash operates periodically, upon expiration of an elapsed time value, to compute a hash value over each of a plurality of segments of each data stream;

the means for combining, the means for hashing, and the means for digitally signing all operate on the periodically-computed hash values for each data stream; and

the means for providing provides the digitally signed periodically-computed hash values, along with the periodically-computed hash values, as the digital notarization; and

further comprising means for inserting an identification of a time corresponding to each of the periodically-computed hash values at appropriate locations within each of the data streams.

16. The system according to Claim 15, wherein the means for inserting uses MPEG-4 synchronization timestamping.

17. The system according to Claim 15, wherein integrity of each of the segments is independently verifiable.

18. The system according to Claim 15, further comprising:

means for extracting selected ones of the segments of the data streams; and

means for verifying integrity of the extracted selected ones using the public cryptographic key of the digital notary.

19. The system according to Claim 15, further comprising:

means for authenticating, by the digital notary, each of the application processing components;

means for extracting selected ones of the segments of the data streams; and

means for verifying authenticity of the extracted selected ones using the public cryptographic key of the digital notary and the digital notarization.

20. The system according to Claim 13, further comprising means for adding an additional data stream to the collection, wherein the additional data stream comprises the digital notarization.

21. The system according to Claim 19, wherein the identifiers serve to identify data streams from each of the authenticated application processing components.

22. The system according to Claim 13, further comprising means for authenticating each of the application processing components using the unique identifier thereof, along with a digital signature of the unique identifier that is created using a private key of the application processing component.

23. The system according to Claim 22, wherein inclusion of the unique identifiers within the combination data block allows concluding that each data stream in the collection was created by an authentic application processing component if operation of a verification process succeeds, wherein the verification process further comprises:

using the public cryptographic key of the digital notary to decrypt the digitally signed hashed combination data block, yielding a new version of the hashed combination data block and a new version of the combination data block;

computing a new hash over the new version of the combination data block; and

determining whether the new hash is identical to the new version of the hashed combination data block.

24. The system according to Claim 23, wherein successful operation of the verification process also allows concluding that the data streams in the collection have not been altered.

25. A method of digitally notarizing a collection comprising a plurality of data streams, comprising steps of:

computing a hash value over each of the plurality of data streams, wherein each data stream is created by a different application processing component;

combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a combination data block;

hashing the combination data block;

digitally signing the hashed combination data block with a private cryptographic key, wherein the private cryptographic key and a public cryptographic key which is cryptographically associated therewith represent a digital notary; and

providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the collection of data streams, wherein the digital notarization cryptographically seals contents of the collection of data streams.

26. The method according to Claim 25, wherein:

the combining step and the hashing step operate on pairs of (hash values, identifiers), one pair for each of the plurality of data streams;

the digitally signing step digitally signs each of the hashed pairs; and

the providing step provides the digitally signed hashed pairs, along with the hashed pairs, as the digital notarization.

27. The method according to Claim 25, wherein:

the step of computing a hash operates periodically, upon expiration of an elapsed time value, to compute a hash value over each of a plurality of segments of each data stream;

the combining step, the hashing step, and the digitally signing step all operate on the periodically-computed hash values for each data stream; and

the providing step provides the digitally signed periodically-computed hash values, along with the periodically-computed hash values, as the digital notarization; and

further comprising the step of inserting an identification of a time corresponding to each of the periodically-computed hash values at appropriate locations within each of the data streams.

28. The method according to Claim 27, wherein the inserting step uses MPEG-4 synchronization timestamping.

29. The method according to Claim 27, wherein integrity of each of the segments is independently verifiable.

30. The method according to Claim 27, further comprising the steps of:

extracting selected ones of the segments of the data streams; and

verifying integrity of the extracted selected ones using the public cryptographic key of the digital notary.

31. The method according to Claim 27, further comprising the steps of:

authenticating, by the digital notary, each of the application processing components;

extracting selected ones of the segments of the data streams; and

verifying authenticity of the extracted selected ones using the public cryptographic key of the digital notary and the digital notarization.

32. The method according to Claim 25, further comprising the step of adding an additional data stream to the collection, wherein the additional data stream comprises the digital notarization.

33. The method according to Claim 31, wherein the identifiers serve to identify data streams from each of the authenticated application processing components.

34. The method according to Claim 25, further comprising the step of authenticating each of the application processing components using the unique identifier thereof, along with a digital signature of the unique identifier that is created using a private key of the application processing component.

35. The method according to Claim 34, wherein inclusion of the unique identifiers within the combination data block allows concluding that each data stream in the collection was created by an authentic application processing component if operation of a verification process succeeds, wherein the verification process further comprises:

using the public cryptographic key of the digital notary to decrypt the digitally signed hashed combination data block, yielding a new version of the hashed combination data block and a new version of the combination data block;

computing a new hash over the new version of the combination data block; and

determining whether the new hash is identical to the new version of the hashed combination data block.

36. The method according to Claim 35, wherein successful operation of the verification process also allows concluding that the data streams in the collection have not been altered.

37. A digitally notarized collection of data streams, comprising:

a plurality of data streams in the collection, wherein each data stream is created by a different application processing component; and

a digital notarization of the collection, created by the steps of:

computing a hash value over each of each of the plurality of data streams;

combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a combination data block;

hashing the combination data block;

digitally signing the hashed combination data block with a private cryptographic key, wherein the private cryptographic key and a public cryptographic key which is cryptographically associated therewith represent a digital notary; and

providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the collection of data streams, wherein the digital notarization cryptographically seals contents of the collection of data streams.

38. A method of doing business using digitally notarized data streams, comprising steps of:

digitally notarizing a collection comprising a plurality of data streams, further comprising steps of:

computing a hash value over each of the plurality of data streams, wherein each data stream is created by a different application processing component;

combining each hash value with a unique identifier of the application processing component which created the data stream for which the hash value was computed, thereby creating a combination data block;

hashing the combination data block;

digitally signing the hashed combination data block with a private cryptographic key, wherein the private cryptographic key and a public cryptographic key which is cryptographically associated therewith represent a digital notary; and

providing the digitally signed hashed combination data block, along with the combination data block, as the digital notarization for the collection of data streams; and

verifying authenticity of the digitally notarized collection of data streams, by a receiver of the digital notarization, further comprising:

using the public cryptographic key of the digital notary to decrypt the digitally signed hashed combination data block, yielding a new version of the hashed combination data block and a new version of the combination data block;

computing a new hash over the new version of the combination data block; and

determining whether the new hash is identical to the new version of the hashed combination data block, and if so, concluding that the data streams in the collection have not been altered.